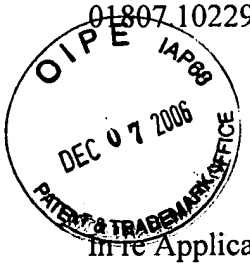
IFW

01807.102296. PATENT APPLICATION



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	:	Examiner: F. Alphonse
PHILIPPE PIRET ET AL.	)	
	:	Art Unit: 2133
Application No.: 10/825,283	)	
	:	
Filed: April 16, 2004	)	
	:	
For: INFORMATION CODING BY ALGEBRAIC GEOMETRIC CODE OFFERING TWO DECODING OPTIONS	) :)	
	:	December 5, 2006

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBMISSION OF PRIORITY DOCUMENT

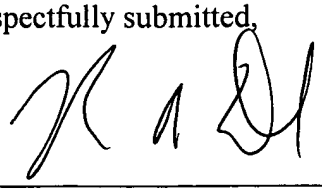
Sir:

In support of Applicants' claim for priority under 35 U.S.C. § 119, enclosed is a certified copy of the following French application:

FR 0304766, filed April 16, 2003.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our address given below.

Respectfully submitted,



Raymond A. DiPerna
Attorney for Applicants
Registration No.: 44,063

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3800
Facsimile: (212) 218-2200

NY_MAIN 502183v1

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

A.N. 10/825,283
GAU 2133

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

CERTIFIED COPY OF PRIORITY DOCUMENT

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 20 AVR. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*03

REQUÊTE EN DÉLIVRANCE page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 e W / 210502

Réservé à l'INPI

REMISE DES PIÈCES
DATE 16 AVRIL 2003
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0304766
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 16 AVR. 2003

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

SANTARELLI
14 avenue de la Grande Armée
75017 PARIS

Vos références pour ce dossier *(facultatif)* BIF023276/DM/LJH

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE — **Cochez l'une des 4 cases suivantes**

Demande de brevet	☒	
Demande de certificat d'utilité	☐	
Demande divisionnaire	☐	
Demande de brevet initiale	N°	Date
ou demande de certificat d'utilité initiale	N°	Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N°	Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Codage d'informations par code de géométrie algébrique offrant deux options de décodage.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases) ☒ **Personne morale** ☐ **Personne physique**

Nom ou dénomination sociale		CANON KABUSHIKI KAISHA
Prénoms		
Forme juridique		Société de droit Japonais
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	3-30-2, Shimomaruko 3-chome, Ohta-ku,
	Code postal et ville	TOKYO
	Pays	JAPON
Nationalité		JAPONAISE
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 18 AVRIL 2003
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0304766

DB 540 W / 210502

6 MANDATAIRE *(s'il y a lieu)*		
Nom		
Prénom		
Cabinet ou Société		SANTARELLI
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	14 avenue de la Grande Armée
	Code postal et ville	7 5 0 1 7 PARIS
	Pays	FRANCE
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG**
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		☐ Cochez la case si la description contient une liste de séquences
Le support électronique de données est joint		☐
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		☐
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
Bruno QUANTIN N°92-1366
SANTARELLI

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

La présente invention concerne les systèmes de communication dans lesquels, afin d'améliorer la fidélité de la transmission, les données à transmettre sont soumises à un codage de canal. Elle concerne plus particulièrement, d'une part, des procédés de codage, et d'autre part des procédés de décodage ainsi que les dispositifs et appareils destinés à mettre en œuvre ces procédés.

On rappelle que le codage dit « de canal » consiste, quand on forme les « mots de code » envoyés au récepteur, à introduire une certaine redondance dans les données à transmettre. Plus précisément, on transmet, au moyen de chaque mot de code, l'information initialement contenue dans un nombre prédéterminé k de symboles prélevés dans un « alphabet » de taille finie q ; on calcule à partir de ces k symboles d'information un nombre n de symboles appartenant à cet alphabet, de manière à former des mots de code $\underline{v} = \left(v^0, v^1, \ldots, v^{n-1}\right)$. L'ensemble des mots de code obtenus quand chaque symbole d'information prend une valeur quelconque dans l'alphabet, constitue une sorte de dictionnaire appelé « code » de « dimension » k et de « longueur » n.

Lorsque la taille q de l'alphabet est une puissance d'un nombre premier, on peut donner à cet alphabet une structure de corps, dit « corps de Galois », noté $\mathbf{F}_q$, dont les éléments non-nuls peuvent être commodément identifiés comme étant chacun égal à γ^{i-1} pour une valeur correspondante de i, où $i = 1, \ldots, q-1$, et où γ est un élément de $\mathbf{F}_q$ choisi parmi les éléments dits « primitifs » de ce corps. Dans le cas où l'alphabet est un corps de Galois, certains codes peuvent, de façon commode, être associés à une matrice H de dimension $(n-k)\times n$ définie sur $\mathbf{F}_q$, dite « matrice de parité » : un mot $\underline{v}$ de longueur n donné est un mot de code si, et seulement si, il vérifie la relation : $H \cdot \underline{v}^{\mathrm{T}} = 0$ (où l'exposant T indique la transposition) ; on dit alors que le code est « orthogonal » à cette matrice H. Ces codes, que l'on appelle « codes linéaires », seront les seuls codes considérés plus bas.

Au niveau du récepteur, le procédé de décodage associé exploite alors judicieusement cette redondance pour détecter d'éventuelles erreurs de

transmission et si possible les corriger. Il y a erreur de transmission si la différence $\underline{e}$ entre un mot reçu $\underline{r}$ et le mot de code $\underline{v}$ correspondant envoyé par l'émetteur, est non-nulle.

Plus précisément, le décodage se fait en deux étapes principales.

La première étape consiste à associer au mot reçu un « mot de code associé ». Pour ce faire, le décodeur calcule d'abord le vecteur de « syndromes d'erreurs » $H \cdot \underline{r}^{\mathrm{T}} = H \cdot \underline{e}^{\mathrm{T}}$. Si les syndromes sont tous nuls, on supposera qu'il n'y a pas eu d'erreur de transmission, et le « mot de code associé » sera alors simplement pris égal au mot reçu. Si ce n'est pas le cas, on en déduit que certains symboles dans le mot reçu sont erronés, et l'on met alors en œuvre un algorithme de correction destiné à estimer la valeur de l'erreur $\underline{e}$; l'algorithme va ainsi fournir une valeur estimée $\underline{\hat{e}}$ de manière à ce que $(r - \underline{\hat{e}})$ soit un mot de code, qui constituera alors le « mot de code associé ».

La seconde étape consiste simplement à inverser le procédé de codage. Dans la situation idéale où toutes les erreurs de transmission ont été corrigées, on retrouve ainsi les symboles d'information initiaux.

Un algorithme de correction d'erreurs a pour tâche d'associer au mot reçu le mot de code situé à la distance de Hamming la plus courte de ce mot reçu, la « distance de Hamming » étant, par définition, le nombre d'emplacements où deux mots de même longueur possèdent un symbole différent. On appelle « distance minimale » *d* d'un code la plus petite distance de Hamming entre deux mots différents de ce code. C'est un paramètre important du code. Plus précisément, il est en principe possible de trouver la position des erreurs éventuelles dans un mot reçu, et de fournir le symbole de remplacement correct (c'est-à-dire, identique à celui envoyé par l'émetteur) pour chacune de ces positions, chaque fois que le nombre de positions erronées est au plus égal à INT[(*d*-1)/2] (où « INT » désigne la partie entière) pour un code de distance minimale *d* (pour certaines configurations d'erreurs, on peut même parfois faire mieux). Dans tous les cas toutefois, il ne s'agit que d'une possibilité de principe, car il est souvent difficile de mettre au point un algorithme de décodage atteignant cette performance. On notera également

que, lorsque l'algorithme choisi parvient à proposer une correction pour le mot reçu, cette correction est d'autant plus fiable (du moins, pour la plupart des canaux de transmission) qu'elle concerne un plus petit nombre de positions.

La capacité d'un algorithme de correction d'erreurs à pouvoir proposer une correction d'un mot reçu est fidèlement représentée par la formule :

$$2\varepsilon \leq \Delta,$$

où ε est le nombre de symboles erronés dans le mot reçu, et Δ est un entier strictement positif que nous appellerons le « pouvoir de résolution » de l'algorithme. Si la valeur de (2ε) est inférieure ou égale au pouvoir de résolution, l'algorithme de correction sera capable de corriger le mot reçu. Si la valeur de (2ε) est supérieure au pouvoir de résolution, l'algorithme pourra :

- soit échouer purement et simplement dans sa tentative de correction,
- soit être capable de proposer une correction du mot reçu ; dans ce cas, si l'on accepte cette correction, on s'expose au risque qu'elle soit erronée, c'est-à-dire que le mot de code proposé ne soit pas, en fait, le mot envoyé, ce risque étant évidemment d'autant plus prononcé que (2ε) est grand par rapport à Δ.

Compte tenu des considérations ci-dessus concernant la distance minimale d du code, on dira que l'algorithme considéré est « maximal » si

$$\Delta = d - 1,$$

et « sub-maximal » si

$$\Delta < d - 1.$$

Parmi les codes connus, on peut citer les « codes de Reed-Solomon », qui sont réputés pour leur efficacité (pour une définition des codes de Reed-Solomon, on pourra se référer à l'ouvrage de R.E. Blahut intitulé « *Theory and practice of error-control codes* », Addison-Wesley, Reading, Mass.,1983). Ces codes sont définis sur $\mathbf{F}_q$, et leur distance minimale d est égale à $(n-k+1)$. Pour leur décodage, on utilise habituellement un algorithme dit de « Berlekamp-Massey » pour la détection des positions erronées dans un mot reçu, et un algorithme dit de « Forney » pour la correction des symboles

erronés correspondants (ces algorithmes sont décrits dans l'ouvrage mentionné ci-dessus).

Dans les supports d'information modernes, par exemple dans les disques durs d'ordinateurs, les CD (« *compacts discs* ») ou encore les DVD (« *digital video discs* »), on cherche à accroître la densité d'information. Quand un tel support est affecté par un défaut physique tel qu'une éraflure, un nombre important de symboles d'information peuvent être rendus illisibles. On peut toutefois remédier à ce problème en utilisant un code de très grande longueur. Or les codes de Reed-Solomon présentent la particularité que la longueur n des mots de code est nécessairement inférieure ou égale à la taille q de l'alphabet des symboles. En fait, quand on cherche, pour q fixé, à maximiser la longueur du code de Reed-Solomon, on pourra préférer prendre une longueur n égale à $(q-1)$ plutôt qu'égale à q : en effet, ainsi qu'il est expliqué dans l'ouvrage de R.E. Blahut cité ci-dessus, il est plus simple de décoder un code de Reed-Solomon de longueur $(q-1)$ défini sur $\mathbf{F}_q$ qu'un code de longueur q (toujours défini sur $\mathbf{F}_q$), de sorte que cette légère perte de longueur est compensée par un gain en facilité de décodage ; dans ce cas, la matrice de parité $H^{(t)}$, où $t = n-k$, du code de Reed-Solomon est une matrice à t lignes et à $(q-1)$ colonnes, qui peut être définie en prenant $H^{(t)}_{ij} = \gamma^{i(j-1)}$ ($1 \leq i \leq t$, $1 \leq j \leq q-1$), où γ est un élément primitif de $\mathbf{F}_q$.

Par conséquent, si l'on souhaite disposer d'un code de Reed-Solomon ayant des mots de code de grande longueur, on doit envisager de grandes valeurs de q, ce qui conduit à des mises en œuvre coûteuses au niveau des calculs et de la mémorisation. De plus, de grandes valeurs de q sont parfois inadaptées à l'application technique envisagée. C'est pourquoi l'on a cherché à construire des codes offrant de manière naturelle une plus grande longueur de mots que les codes de Reed-Solomon.

On a notamment proposé récemment des codes dits « codes de géométrie algébrique » ou « codes de Goppa géométriques » (voir par exemple « *Algebraic Geometric Codes* », par J.H. van Lint, dans « *Coding Theory and Design Theory* », 1ère partie, *IMA Volumes Math. Appl.*, volume 21, Springer-Verlag, Berlin, 1990). Ces codes, eux aussi définis sur un corps de Galois $\mathbf{F}_q$,

sont construits à partir d'une équation algébrique à deux inconnues X et Y. Les solutions de cette équation algébrique peuvent être considérées comme les coordonnées (x,y) de points d'une « courbe algébrique ». Pour définir une matrice de parité, on constitue d'abord un ensemble ordonné, appelé « ensemble de localisation » (« *locating set* » en anglais), à partir de n tels points dont toutes les coordonnées sont finies ; puis chaque ligne de la matrice de parité est obtenue en évaluant une fonction bien choisie de X et Y en chaque élément de cet ensemble de localisation. On obtient ainsi un code de géométrie algébrique de longueur n.

Un paramètre important d'une telle courbe est son « genre » g. Dans le cas particulier où la courbe est une simple droite (le genre g est alors nul), le code de géométrie algébrique se réduit à un code de Reed-Solomon. Dans certains cas, les codes de géométrie algébrique permettent d'atteindre une longueur égale à $\left(q+2g\sqrt{q}\right)$, qui peut être très élevée ; par exemple, avec une taille d'alphabet égale à 256 et un genre égal à 120, on obtient des mots de code de longueur 4096. On notera par ailleurs que les codes de géométrie algébrique possèdent une distance minimale d supérieure ou égale à $(n-k+1-g)$.

Comme tous les codes, les codes de géométrie algébrique peuvent être « raccourcis ». On dit qu'un code donné est une version « raccourcie » du code C s'il ne comprend que les mots de C dont, pour un nombre R de positions prédéterminées, les composantes sont toutes nulles : ces positions étant connues du récepteur, on peut se dispenser de les transmettre, de sorte que le code raccourci est de longueur $(n-R)$. En particulier, il est courant de raccourcir un code de géométrie algébrique en supprimant de l'ensemble de localisation, le cas échéant, un point, ou plusieurs points, dont la coordonnée x est nulle.

Les codes de géométrie algébrique sont avantageux quant à leur distance minimale et, comme on l'a dit, quant à la longueur des mots de code, mais ils présentent l'inconvénient de requérir des algorithmes de décodage assez complexes, et donc assez coûteux en termes d'équipements (logiciel et/ou matériel) et de temps de traitement. Cette complexité est en fait plus ou

moins grande selon l'algorithme considéré, une plus grande complexité étant en principe le prix à payer pour accroître la capacité de correction d'erreurs du décodeur (voir par exemple l'article de Tom Høholdt et Ruud Pellikaan intitulé « *On the Decoding of Algebraic-Geometric Codes* », *IEEE Trans. Inform. Theory*, vol. 41 n° 6, pages 1589 à 1614, novembre 1995).

L'invention a pour but, *inter alia*, de proposer un code permettant de corriger un nombre relativement élevé d'erreurs de transmission de manière économique.

L'invention concerne ainsi, selon un premier aspect, un procédé de codage de symboles d'information selon un code défini sur un corps de Galois $\mathbf{F}_q$, où q est un entier supérieur à 2 et égal à une puissance d'un nombre premier, et de longueur $n = p(q-1)$, où p un entier supérieur à 1, ledit procédé étant remarquable en ce qu'il comprend les étapes suivantes :

a) on choisit un p-uple d'entiers $(t_1,\ldots,t_p)$ tels que

$$q-1 > t_1 > t_2 > \ldots > t_p > 0 ,$$

et un p-uple de matrices carrées diagonales $(Y_1,\ldots,Y_p)$ de dimension $(q-1)$ sur $\mathbf{F}_q$ telles que, pour tout i $(1 \leq i \leq q-1)$, les p éléments en position (i,i) de ces matrices $Y_1,\ldots,Y_p$ sont différents deux à deux,

b) on place lesdits symboles d'information successivement dans p mots $\underline{a}_l$ de longueur $(q-1-t_l)$ (où $l = 1,\ldots,p$),

c) on forme des mots $\underline{u}_l$ (où $l = 1,\ldots,p$) de longueur $(q-1)$, qui constituent les composantes du « mot pré-codé » $\underline{u} = [\underline{u}_1\ \underline{u}_2\ \ldots\ \underline{u}_p]$, en complétant le mot $\underline{a}_l$ correspondant au moyen de symboles de redondance de manière à ce que $\underline{u}_l$ soit orthogonal à la matrice $H^{(t_l)}$, où les matrices $H^{(t)}$ sont définies par $H^{(t)}_{ij} = \gamma^{i(j-1)}$ $(1 \leq i \leq t,\ 1 \leq j \leq q-1)$, où γ est un symbole choisi parmi les éléments primitifs de $\mathbf{F}_q$, et

d) on forme un mot de code

$$\underline{v} = [\underline{v}_1\ \underline{v}_2\ \ldots\ \underline{v}_p] ,$$

où chaque mot $\underline{v}_l$ $(l = 1,\ldots,p)$ est de longueur $(q-1)$, en résolvant le système d'équations

$$\begin{cases} \underline{v}_1 + \underline{v}_2 + \ldots + \underline{v}_p = \underline{u}_1 , \\ \underline{v}_1 Y_1 + \underline{v}_2 Y_2 + \ldots + \underline{v}_p Y_p = \underline{u}_2 , \\ \underline{v}_1 Y_1^2 + \underline{v}_2 Y_2^2 + \ldots + \underline{v}_p Y_p^2 = \underline{u}_3 , \\ \qquad\qquad \ldots \\ \underline{v}_1 Y_1^{p-1} + \underline{v}_2 Y_2^{p-1} + \ldots + \underline{v}_p Y_p^{p-1} = \underline{u}_p . \end{cases}$$

Corrélativement, l'invention concerne, selon le même premier aspect, un procédé de décodage de données reçues résultant de la transmission de symboles codés de la manière décrite succinctement ci-dessus, ledit procédé étant remarquable en ce qu'il comprend les étapes suivantes :

e) on calcule, à partir du mot reçu

$$\underline{r} = [\underline{r}_1 \; \underline{r}_2 \cdots \underline{r}_p] ,$$

où chaque mot $\underline{r}_l$ (l = 1,...,p) est de longueur (q−1), au moins une des composantes $\underline{s}_l$ (où l = 1,...,p) de longueur (q−1), du « mot post-reçu » $\underline{s} = [\underline{s}_1 \; \underline{s}_2 \cdots \underline{s}_p]$, d'après :

$$\begin{cases} \underline{s}_1 = \underline{r}_1 + \underline{r}_2 + \ldots + \underline{r}_p , \\ \underline{s}_2 = \underline{r}_1 Y_1 + \underline{r}_2 Y_2 + \ldots + \underline{r}_p Y_p , \\ \underline{s}_3 = \underline{r}_1 Y_1^2 + \underline{r}_2 Y_2^2 + \ldots + \underline{r}_p Y_p^2 , \\ \qquad\qquad \ldots \\ \underline{s}_p = \underline{r}_1 Y_1^{p-1} + \underline{r}_2 Y_2^{p-1} + \ldots + \underline{r}_p Y_p^{p-1} , \end{cases}$$

et

f) on calcule au moins une des composantes $\hat{\underline{u}}_l$ (où l = 1,...,p), de longueur (q−1), du « mot post-associé » $\hat{\underline{u}} = [\hat{\underline{u}}_1 \hat{\underline{u}}_2 \ldots \hat{\underline{u}}_p]$, en corrigeant le mot $\underline{s}_l$ de même l d'après le vecteur de syndromes d'erreurs $H^{(t_l)} \cdot \underline{s}_l{}^{\mathrm{T}}$.

Ainsi, la correction d'erreurs de transmission dans les mots codés selon l'invention est essentiellement ramenée à la correction d'erreurs dans p mots codés selon Reed-Solomon. La correction d'erreurs pour chacune de ces p composantes est relativement simple et rapide en vertu des qualités des algorithmes connus adaptés aux codes de Reed-Solomon, et ce d'autant plus que l'on corrige des mots de longueur (q−1) définis sur $\mathbf{F}_q$, comme expliqué ci-dessus.

Selon des caractéristiques particulières, on considère une équation algébrique en X et Y telle que, pour toute valeur γ^{i-1} (i = 1,...,q−1) prise par X, ladite équation algébrique possède p solutions distinctes notées $y_l(\gamma^{i-1})$ (où l = 1,...,p), et l'élément diagonal en position (i,i) de chacune desdites matrices Y_l est pris égal à $y_l(\gamma^{i-1})$.

Dans ce cas, le code selon l'invention est un code de géométrie algébrique, orthogonal à la matrice de parité :

$$H = \begin{bmatrix} H^{(t_1)} & H^{(t_1)} & \dots & H^{(t_1)} \\ H^{(t_2)}Y_1 & H^{(t_2)}Y_2 & \dots & H^{(t_2)}Y_p \\ H^{(t_3)}Y_1^2 & H^{(t_3)}Y_2^2 & \dots & H^{(t_3)}Y_p^2 \\ & & \dots & \\ H^{(t_p)}Y_1^{p-1} & H^{(t_p)}Y_2^{p-1} & \dots & H^{(t_p)}Y_p^{p-1} \end{bmatrix}.$$

Ce choix particulier offre plusieurs avantages supplémentaires. Trois d'entre eux méritent particulièrement d'être mentionnés. En premier lieu, on bénéficie de la grande distance minimale garantie par les codes de géométrie algébrique.

En second lieu, on connaît, pour ces codes, des algorithmes de corrections d'erreurs, tels que l'algorithme de Feng-Rao, aptes à tirer le meilleur parti possible de cette grande distance minimale (bien que la distance minimale du code selon l'invention ne soit pas toujours exactement connue, on considérera que l'algorithme de Feng-Rao est, en pratique, « maximal » au sens défini ci-dessus). Ainsi, corrélativement, l'invention concerne un procédé de décodage de données reçues résultant de la transmission de symboles codés selon le mode de réalisation particulier décrit succinctement ci-dessus, ledit procédé étant remarquable en ce qu'il comprend les étapes suivantes :

e') on applique à chaque mot reçu $\underline{r}$ un algorithme de correction d'erreurs maximal, de manière à obtenir une estimation

$$\underline{\hat{v}} = [\underline{\hat{v}}_1\ \underline{\hat{v}}_2\ \dots\ \underline{\hat{v}}_p]\ ,$$

où chaque mot $\underline{\hat{v}}_l$ (l = 1,...,p) est de longueur (q−1), du mot transmis $\underline{v}$ correspondant, et

f') on calcule au moins une des composantes $\underline{\hat{u}}_l$ (où l = 1,...,p), de longueur (q−1), du « mot post-associé » $\underline{\hat{u}} = [\underline{\hat{u}}_1 \underline{\hat{u}}_2 ... \underline{\hat{u}}_p]$, d'après :

$$\begin{cases} \underline{\hat{u}}_1 = \underline{\hat{v}}_1 + \underline{\hat{v}}_2 + \ldots + \underline{\hat{v}}_p , \\ \underline{\hat{u}}_2 = \underline{\hat{v}}_1 Y_1 + \underline{\hat{v}}_2 Y_2 + \ldots + \underline{\hat{v}}_p Y_p , \\ \underline{\hat{u}}_3 = \underline{\hat{v}}_1 Y^2_1 + \underline{\hat{v}}_2 Y^2_2 + \ldots + \underline{\hat{v}}_p Y^2_p , \\ \qquad\qquad \ldots \\ \underline{\hat{u}}_p = \underline{\hat{v}}_1 Y^{p-1}_1 + \underline{\hat{v}}_2 Y^{p-1}_2 + \ldots + \underline{\hat{v}}_p Y^{p-1}_p . \end{cases}$$

En troisième lieu, on notera que l'homme du métier choisit habituellement tel codage/décodage plutôt qu'un autre, en fonction, notamment, du cahier des charges (coût, fiabilité) de l'application envisagée. Mais ce choix s'avère être difficile dans le cas où cette application concerne un canal dans lequel le niveau de bruit varie de façon importante dans le temps ; de même, un fabricant de dispositifs de codage et de décodage a du mal à fixer les caractéristiques de son produit s'il ne sait pas, au stade de la fabrication, si ce produit sera mis en œuvre ultérieurement dans des canaux de bruit élevé ou faible. En effet, on se trouve devant le dilemme suivant : si le procédé de décodage comporte un algorithme de correction d'erreurs performant, celui-ci s'avèrera être trop coûteux si, une fois la transmission commencée, on constate que le taux d'erreurs de transmission est nettement plus faible que prévu ; si en revanche le procédé de décodage comporte un algorithme de correction d'erreurs économique, mais moyennement performant, la transmission souffrira d'un taux excessif d'erreurs non corrigées si, une fois la transmission commencée, on constate que le taux d'erreurs de transmission est nettement plus élevé que prévu.

Le mode de réalisation de l'invention succinctement décrit ci-dessus résout ce problème en permettant de corriger les mots reçus, au choix, soit en mettant en œuvre un algorithme maximal, soit en mettant en œuvre l'algorithme sub-maximal, décrit succinctement ci-dessus, faisant appel à p algorithmes adaptés aux codes de Reed-Solomon (on dira que l'on applique au mot reçu courant, respectivement, soit un « procédé de décodage maximal », soit un « procédé de décodage sub-maximal »). Cet avantage du code de géométrie algébrique selon l'invention pourra éventuellement, d'ailleurs, s'étendre au code

selon l'invention dans sa forme la plus générale, telle que décrite succinctement ci-dessus, s'il s'avère qu'il existe un algorithme de correction d'erreurs maximal adapté à ce code.

On peut, en pratique, faire usage de cet avantage de diverses manières.

Ainsi, selon des caractéristiques particulières, le procédé de décodage pourra comprendre une étape préliminaire consistant à choisir, pour le mot reçu courant, entre les étapes du procédé de décodage « sub-maximal », et les étapes du procédé de décodage « maximal », tels que décrites succinctement ci-dessus, en fonction de critères prédéterminés, par exemple une estimation du bruit du canal.

Selon d'autres caractéristiques particulières, le procédé de décodage pourra, pour tout mot reçu, mettre d'abord en œuvre les étapes du « procédé sub-maximal », et, au cas où ce procédé n'aboutit pas, déclarer qu'une erreur non corrigible a été détectée, et/ou mettre ensuite en œuvre les étapes du « procédé maximal ». En effet, comme mentionné ci-dessus, un algorithme de correction d'erreurs peut s'avérer être incapable de proposer un mot corrigé quand le nombre d'erreurs est trop élevé eu égard à son pouvoir de résolution.

Quel que soit le procédé de décodage, tel que décrit succinctement ci-dessus, utilisé, on pourra ensuite obtenir des symboles d'information estimés en ôtant d'au moins une composante $\underline{\hat{u}}_l$ (l = 1,...,p) les symboles situés aux positions identiques aux positions de la composante $\underline{u}_l$ de même l du mot pré-codé $\underline{u}$ correspondant, dans lesquelles des symboles de redondance ont été placés à l'étape c) du codage selon l'invention. On obtient ainsi une estimation des symboles d'information contenus dans le mot $\underline{a}_l$ correspondant.

On notera à cet égard que l'invention offre, commodément, la possibilité de ne décoder que les symboles d'information contenus dans certains des mots formant le bloc $\underline{a}$, ce qui peut être économiquement avantageux pour certaines applications. C'est par exemple le cas lorsque l'information à transmettre représente des images codées à la source selon une série d'approximations de résolutions différentes. Ainsi, dans le procédé de

codage à la source appelé « décomposition en sous-bandes », on divise chaque image à transmettre en plusieurs blocs de données (appelés « sous-bandes ») hiérarchisés, et cela de façon itérative ; par exemple, à la première itération, on crée quatre sous-bandes : la première contient les fréquences basses de l'image, la deuxième les hautes fréquences horizontales, la troisième les hautes fréquences verticales et la quatrième les hautes fréquences diagonales, chaque sous-bande contenant quatre fois moins de données (pixels) que l'image originale ; à la deuxième itération, la sous-bande basses fréquences est elle-même décomposée en quatre nouveaux blocs contenant les basses fréquences, les hautes fréquences horizontales, les hautes fréquences verticales et les fréquences diagonales relatives à cette sous-bande ; on poursuit ainsi le processus de décomposition un certain nombre de fois selon les besoins. Au cours du codage de canal selon l'invention, on peut alors faire correspondre le mot $\underline{a}_1$ aux fréquences d'image les plus basses (qui contribuent le plus à l'intelligibilité de l'image, et nécessitent donc la plus grande protection vis-à-vis des erreurs de transmission), le mot $\underline{a}_2$ aux fréquences plus élevées, le mot $\underline{a}_3$ aux fréquences encore plus élevées, et ainsi de suite ; on pourra alors, selon la qualité de service requise par le système de communication ou par le destinataire des images, ne calculer que la composante $\hat{\underline{u}}_1$ du mot post-associé, ou ne calculer que les composantes $\hat{\underline{u}}_1$ et $\hat{\underline{u}}_2$, ou ne calculer que les composantes $\hat{\underline{u}}_1$, $\hat{\underline{u}}_2$ et $\hat{\underline{u}}_3$, et ainsi de suite, avant d'en extraire les symboles d'information estimés correspondants. On trouve un autre exemple d'application dans le codage d'images à la source selon la méthode dite « par ondelettes », telle que définie par la norme JPEG-2000.

L'invention concerne également, selon le même premier aspect, un procédé de communication de symboles d'information comprenant les étapes suivantes :

1) on code lesdits symboles d'information conformément à l'un des procédés de codage succinctement décrits ci-dessus, de façon à former des mots de code $\underline{v} = \left(v^0, v^1, \ldots, v^{n-1}\right)$,

2) on permute les symboles de chaque mot de code $\underline{v}$ de façon à former un mot à transmettre

$$\underline{v}^* = \left(v^0, v^{q-1}, v^{2(q-1)}, \ldots, v^{(p-1)(q-1)}, v^1, v^q, v^{2q-1}, \ldots, v^{(p-1)(q-1)+1}, \ldots, v^{n-1}\right),$$

3) on transmet ledit mot $\underline{v}^*$,

4) on reçoit un mot entrelacé

$$\underline{r}^* = \left(r^0, r^{q-1}, r^{2(q-1)}, \ldots, r^{(p-1)(q-1)}, r^1, r^q, v^{2q-1}, \ldots, r^{(p-1)(q-1)+1}, \ldots, r^{n-1}\right),$$

correspondant au mot $\underline{v}^*$,

5) on permute les symboles du mot entrelacé $\underline{r}^*$ de façon à former un mot reçu $\underline{r} = \left(r^0, r^1, \ldots, r^{n-1}\right)$, et

6) on décode le mot reçu $\underline{r}$ conformément à l'un des procédés de décodage succinctement décrits ci-dessus, adapté audit procédé de codage.

Outre les avantages des procédés de codage et de décodage correspondants, ce procédé de communication offre, de par la combinaison d'un entrelacement et d'un désentrelacement inverse de cet entrelacement, une limitation de la propagation d'erreurs en cas de rafale d'erreurs (en anglais, « *error burst* ») durant la transmission des symboles codés (on rappelle qu'une rafale est une série d'erreurs de fréquence élevée par rapport à la fréquence d'erreurs moyenne sur le canal considéré ; on observe de telles rafales aussi bien sur certaines transmissions hertziennes que sur certains enregistrements sur disque dur). En effet, une rafale d'erreurs affectant bp symboles de $\underline{v}^*$ en cours de transmission affectera au plus $(b+1)$ symboles dans chacun des mots $\underline{u}_l$ (où $l = 1,\ldots,p$), alors que sans entrelacement, chacun de ces mots $\underline{u}_l$ subirait bp erreurs de transmission.

Selon un deuxième aspect, l'invention concerne divers dispositifs.

L'invention concerne ainsi, premièrement, un dispositif de codage de symboles d'information selon un code défini sur un corps de Galois $\mathbf{F}_q$, où q est un entier supérieur à 2 et égal à une puissance d'un nombre premier, et de longueur $n = p(q-1)$, où p un entier supérieur à 1, ledit dispositif étant remarquable en ce que, un p-uple d'entiers $(t_1,\ldots,t_p)$ tels que

$$q-1 > t_1 > t_2 > \ldots > t_p > 0 ,$$

et un p-uple de matrices carrées diagonales $(Y_1,\ldots,Y_p)$ de dimension $(q-1)$ sur $\mathbf{F}_q$ telles que, pour tout i $(1\leq i \leq q-1)$, les p éléments en position (i,i) de ces matrices $Y_1,\ldots,Y_p$ sont différents deux à deux, ayant été choisis, il est apte :

- à placer lesdits symboles d'information successivement dans p mots $\underline{a}_l$ de longueur $(q-1-t_l)$ (où $l = 1,\ldots,p$),

- à former des mots $\underline{u}_l$ (où $l = 1,\ldots,p$) de longueur $(q-1)$, qui constituent les composantes du « mot pré-codé » $\underline{u} = [\underline{u}_1\ \underline{u}_2\ \ldots\ \underline{u}_p]$, en complétant le mot $\underline{a}_l$ correspondant au moyen de symboles de redondance de manière à ce que $\underline{u}_l$ soit orthogonal à la matrice $H^{(t_l)}$, où les matrices $H^{(t)}$ sont définies par $H^{(t)}_{ij} = \gamma^{i(j-1)}$ $(1\leq i \leq t,\ 1 \leq j \leq q-1)$, où γ est un symbole choisi parmi les éléments primitifs de $\mathbf{F}_q$, et

- à former un mot de code

$$\underline{v} = [\underline{v}_1\ \underline{v}_2\ \ldots\ \underline{v}_p]\ ,$$

où chaque mot $\underline{v}_l$ $(l = 1,\ldots,p)$ est de longueur $(q-1)$, en résolvant le système d'équations

$$\begin{cases} \underline{v}_1 + \underline{v}_2 + \ldots + \underline{v}_p = \underline{u}_1\ , \\ \underline{v}_1 Y_1 + \underline{v}_2 Y_2 + \ldots + \underline{v}_p Y_p = \underline{u}_2\ , \\ \underline{v}_1 Y_1^2 + \underline{v}_2 Y_2^2 + \ldots + \underline{v}_p Y_p^2 = \underline{u}_3\ , \\ \qquad\qquad \ldots \\ \underline{v}_1 Y_1^{p-1} + \underline{v}_2 Y_2^{p-1} + \ldots + \underline{v}_p Y_p^{p-1} = \underline{u}_p\ . \end{cases}$$

Selon des caractéristiques particulières, ce dispositif est en outre apte à assigner la valeur $y_l(\gamma^{i-1})$ à l'élément diagonal en position (i,i) de chacune desdites matrices Y_l, où, pour une équation algébrique en X et Y prédéterminée, ladite équation algébrique possède p solutions distinctes notées $y_l(\gamma^{i-1})$ (où $l = 1,\ldots,p$) pour toute valeur γ^{i-1} $(i = 1,\ldots,q-1)$ prise par X.

L'invention concerne aussi, deuxièmement, un dispositif de décodage de mots reçus $\underline{r}$ résultant de la transmission de mots $\underline{v}$ codés selon l'invention, ledit dispositif étant remarquable en ce qu'il comprend :

- une unité de correction d'erreurs apte à appliquer à chaque mot reçu $\underline{r}$ un algorithme de correction d'erreurs, de manière à fournir au moins une composante $\underline{\hat{u}}_l$ (où $l = 1,\ldots,p$) d'un « mot post-associé » $\underline{\hat{u}}$, et

- une unité de suppression de la redondance apte à ôter de ladite composante $\underline{\hat{u}}_l$ les symboles situés aux positions identiques aux positions de la composante $\underline{u}_l$ de même l du mot pré-codé $\underline{u}$ correspondant, dans lesquelles des symboles de redondance ont été placés lors du codage.

Lorsque le code utilisé est un code de géométrie algébrique selon l'invention, ce dispositif pourra comprendre en outre une unité de sélection capable de déterminer, en fonction de critères prédéterminés, si l'on doit appliquer au mot reçu $\underline{r}$ courant un « procédé de décodage sub-maximal » et/ou un « procédé de décodage maximal » tels que décrits succinctement ci-dessus.

Les avantages de ces dispositifs sont essentiellement les mêmes que ceux des procédés de codage et de décodage correspondants décrits succinctement ci-dessus.

L'invention vise également :

- un appareil de transmission de données d'information comprenant un dispositif de codage tel que décrit succinctement ci-dessus, ainsi qu'un modulateur pour moduler les données résultant du codage desdites données d'information,

- un appareil de réception de données comprenant un démodulateur pour démoduler les données reçues, ainsi qu'un dispositif de décodage tel que décrit succinctement ci-dessus,

- un appareil de transmission de données d'information comprenant un dispositif de codage tel que décrit succinctement ci-dessus, un entrelaceur apte à permuter les symboles de chaque mot de code $\underline{v} = \left(v^0, v^1, \ldots, v^{n-1}\right)$ de façon à former un mot à transmettre

$$\underline{v}^* = \left(v^0, v^{q-1}, v^{2(q-1)}, \ldots, v^{(p-1)(q-1)}, v^1, v^q, v^{2q-1}, \ldots, v^{(p-1)(q-1)+1}, \ldots, v^{n-1}\right),$$

et un modulateur pour moduler les symboles dudit mot à transmettre $\underline{v}^*$,

- un appareil de réception de données comprenant un démodulateur pour démoduler les données reçues de façon à former des mots reçus entrelacés

$$\underline{r}^* = \left(r^0, r^{q-1}, r^{2(q-1)}, \ldots, r^{(p-1)(q-1)}, r^1, r^q, v^{2q-1}, \ldots, r^{(p-1)(q-1)+1}, \ldots, r^{n-1}\right),$$

où q est un entier supérieur à 2 et égal à une puissance d'un nombre premier, p un entier supérieur à 1, et $n = p(q-1)$, un désentrelaceur pour permuter les symboles de chaque mot reçu entrelacé $\underline{r}^*$ de façon à former un mot reçu $\underline{r} = \left(r^0, r^1, \ldots, r^{n-1}\right)$, et un dispositif de décodage tel que décrit succinctement ci-dessus,

- un moyen de stockage de données inamovible comportant des instructions de code de programme informatique pour l'exécution des étapes de l'un quelconque des procédés de codage et/ou de décodage et/ou de communication succinctement exposés ci-dessus,

- un moyen de stockage de données partiellement ou totalement amovible, comportant des instructions de code de programme informatique pour l'exécution des étapes de l'un quelconque des procédés de codage et/ou de décodage et/ou de communication succinctement exposés ci-dessus, et

- un programme d'ordinateur, contenant des instructions telles que, lorsque ledit programme commande un dispositif de traitement de données programmable, lesdites instructions font que ledit dispositif de traitement de données met en œuvre l'un des procédés de codage et/ou de décodage et/ou de communication succinctement exposés ci-dessus.

Les avantages offerts par ces appareils de transmission, ces appareils de réception, ces moyens de stockage de données et ce programme d'ordinateur sont essentiellement les mêmes que ceux offerts par les procédés de codage, de décodage et de communication selon l'invention.

D'autres aspects et avantages de l'invention apparaîtront à la lecture de la description détaillée ci-dessous de modes de réalisation particuliers, donnés à titre d'exemples non limitatifs. La description se réfère aux dessins qui l'accompagnent, dans lesquels :

- la figure 1 est un schéma synoptique d'un système de transmission d'informations selon un mode de réalisation de l'invention,

- la figure 2 représente un appareil d'enregistrement de données d'information comprenant un codeur selon l'invention, et

- la figure 3 représente un appareil de reproduction de données d'information comprenant un décodeur selon l'invention.

La **figure 1** est un schéma synoptique d'un système de transmission d'informations mettant en œuvre un procédé de communication selon un mode de réalisation de l'invention.

Ce système a pour fonction de transmettre des informations de nature quelconque à partir d'une source 100 vers un destinataire ou utilisateur 109. En premier lieu, la source 100 met ces informations sous la forme de symboles appartenant à un certain alphabet (par exemple des octets de bits dans le cas où la taille q de l'alphabet vaut 256), et transmet ces symboles à une unité de stockage 101, qui accumule les symboles de façon à former des ensembles contenant chacun k symboles. Ensuite, chacun de ces ensembles est transmis par l'unité de stockage 101 à une unité de codage 102 qui construit un mot $\underline{v}$ orthogonal à la matrice de parité H.

On va à présent illustrer les procédés de codage et de décodage selon l'invention à l'aide d'un exemple numérique. On notera que cet exemple ne constitue pas nécessairement un choix de paramètres préférentiel pour le codage ou le décodage. Il n'est fourni ici que pour permettre à l'homme du métier de comprendre plus facilement le fonctionnement de l'invention.

Considérons donc un code de géométrie algébrique de longueur 1020 et de dimension 916 défini, de manière classique, comme suit.

L'alphabet des symboles est constitué par les 2^8 éléments du corps de Galois $\mathbf{F}_{256}$ (c'est-à-dire par des octets de symboles binaires) (ce corps peut être construit à l'aide du polynôme $(X^8 + X^4 + X^3 + X^2 + 1)$ défini sur $\mathbf{F}_2$).

On considère alors la courbe algébrique de genre $g = 24$ constituée par l'ensemble des solutions dans $\mathbf{F}_{256}$ de l'équation à deux inconnues

$Y^4 + Y = X^{17}$.

Pour toute valeur prise par X dans $\mathbf{F}_{256}$, les $p = 4$ solutions de l'équation correspondante en Y sont elles aussi dans $\mathbf{F}_{256}$. Ces solutions (X,Y) définissent les « points de la courbe » associée à cette équation sur $\mathbf{F}_{256}$. Cette courbe comprend donc 1024 points de coordonnées finies (ainsi qu'un point à l'infini P_∞). De cet ensemble, on supprime les quatre solutions de l'équation pour lesquelles $X = 0$, afin de construire des codes « raccourcis ». L'ensemble des points P_j (où $j = 1,\ldots,1020$) restants va donc constituer l'ensemble de localisation, chaque point P_j servant à identifier le j-ème élément de tout mot de code.

Ensuite, on considère l'espace vectoriel $L(mP_\infty)$ de polynômes en X et Y à coefficients dans $\mathbf{F}_{256}$ dont les seuls pôles sont situés en P_∞, et sont d'ordre inférieur ou égal à m, où m est un entier strictement positif (il s'agit donc d'un code de géométrie algébrique dit « à un point »). Cet espace vectoriel, qui est de dimension supérieure ou égale à $(m-g+1)$ (égale si $m \geq 2g-2$), possède une base constituée par les monômes (X^rY^s), où r est un entier positif ou nul, s est un entier compris entre 0 et 3, et : $17s + 4r \leq m$.

On définit classiquement une matrice de parité H' de la manière suivante : l'élément en ligne i et colonne j de cette matrice est égal au i-ème monôme de ladite base (avec $1 \leq i \leq m-g+1$) évalué au point P_j (avec $j = 1,\ldots,1020$) de la courbe algébrique. Prenons par exemple : $m = 127$; on obtient alors $n-k = 104$, et donc $k = 916$.

En fait, il nous sera plus commode de définir le code au moyen d'une matrice H un peu différente de H' et qui s'écrit :

$$H = \begin{bmatrix} H^{(32)} & H^{(32)} & H^{(32)} & H^{(32)} \\ H^{(28)}Y_1 & H^{(28)}Y_2 & H^{(28)}Y_3 & H^{(28)}Y_4 \\ H^{(24)}Y_1^2 & H^{(24)}Y_2^2 & H^{(24)}Y_3^2 & H^{(24)}Y_4^2 \\ H^{(20)}Y_1^3 & H^{(20)}Y_2^3 & H^{(20)}Y_3^3 & H^{(20)}Y_4^3 \end{bmatrix}, \qquad (1)$$

où

$$H^{(t)} \equiv \begin{bmatrix} 1 & \gamma & \gamma^2 & \gamma^3 & \cdots & \gamma^{254} \\ 1 & \gamma^2 & \gamma^4 & \gamma^6 & \cdots & \gamma^{253} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \gamma^t & \gamma^{2t} & \gamma^{3t} & \cdots & \gamma^{255-t} \end{bmatrix}, \qquad (2)$$

et chaque matrice Y_l est définie comme étant la matrice carrée diagonale de dimension 255 dont l'élément de position (i,i) est égal à y_l (γ^{i-1}). Le code orthogonal à la matrice H' est différent du code orthogonal à la matrice H, mais il lui est équivalent en ce sens que chaque mot du premier code est identique à un unique mot du second code multiplié par une matrice diagonale Z, de taille 1020 x 1020, telle que $Z_{ii} = \gamma^{i-1}$ $(i = 1,\ldots,1020)$.

On va décrire à présent la façon dont, selon ce mode de réalisation de l'invention, l'unité de codage 102 construit un mot $\underline{v}$ orthogonal à la matrice de parité H ci-dessus.

L'unité de codage 102 forme d'abord des blocs d'information $\underline{a}$ de longueur k = 916 en puisant des symboles successifs dans l'unité de stockage 101, ces blocs $\underline{a}$ étant structurés en quatre mots selon

$$\underline{a} = [\underline{a}_1\ \underline{a}_2\ \underline{a}_3\ \underline{a}_4]\ ,$$

où le mot $\underline{a}_1$ est de longueur 223, le mot $\underline{a}_2$ est de longueur 227, le mot $\underline{a}_3$ est de longueur 231, et le mot $\underline{a}_4$ est de longueur 235.

On forme alors un « mot pré-codé »

$$\underline{u} = [\underline{u}_1\ \underline{u}_2\ \underline{u}_3\ \underline{u}_4]$$

de la façon suivante : on obtient le mot $\underline{u}_1$ de longueur 255 en complétant $\underline{a}_1$ avec des symboles de redondance de façon à ce que :

$$H^{(32)} \cdot \underline{u}_1{}^{\mathrm{T}} = 0\ , \qquad (3a)$$

et le mot $\underline{u}_2$ de longueur 255 en complétant $\underline{a}_2$ avec des symboles de redondance de façon à ce que :

$$H^{(28)} \cdot \underline{u}_2{}^{\mathrm{T}} = 0\ , \qquad (3b)$$

et le mot $\underline{u}_3$ de longueur 255 en complétant $\underline{a}_3$ avec des symboles de redondance de façon à ce que :

$$H^{(24)} \cdot \underline{u}_3{}^{\mathrm{T}} = 0\ , \qquad (3c)$$

et enfin le mot $\underline{u}_4$ de longueur 255 en complétant $\underline{a}_4$ avec des symboles de redondance de façon à ce que :

$$H^{(20)} \cdot \underline{u}_4{}^{\mathrm{T}} = 0\ . \qquad (3d)$$

Considérons alors les mots

$$\underline{v} = [\underline{v}_1\ \underline{v}_2\ \underline{v}_3\ \underline{v}_4] ,$$

où les mots $\underline{v}_1$, $\underline{v}_2$, $\underline{v}_3$, et $\underline{v}_4$ sont tous quatre de longueur 255 et obéissent au système d'équations suivant :

$$\begin{cases} \underline{v}_1 + \underline{v}_2 + \underline{v}_3 + \underline{v}_4 = \underline{u}_1 , \\ \underline{v}_1 Y_1 + \underline{v}_2 Y_2 + \underline{v}_3 Y_3 + \underline{v}_4 Y_4 = \underline{u}_2 , \\ \underline{v}_1 Y_1^2 + \underline{v}_2 Y_2^2 + \underline{v}_3 Y_3^2 + \underline{v}_4 Y_4^2 = \underline{u}_3 , \\ \underline{v}_1 Y_1^3 + \underline{v}_2 Y_2^3 + \underline{v}_3 Y_3^3 + \underline{v}_4 Y_4^3 = \underline{u}_4 . \end{cases} \quad (4)$$

On peut vérifier facilement que ces mots $\underline{v}$ sont orthogonaux à la matrice H de l'équation (1) : il s'agit donc bien de mots de code associés à H.

Les matrices Y_i étant régulières, le système d'équations (4) possède toujours une solution unique, qui est donnée par :

$$\underline{v}_1 K_1 = \underline{u}_1 Y_2 Y_3 Y_4 + \underline{u}_2 (Y_2 Y_3 + Y_3 Y_4 + Y_4 Y_2) + \underline{u}_3 (Y_2 + Y_3 + Y_4) + \underline{u}_4 , \quad (5a)$$

$$\underline{v}_2 K_2 = \underline{u}_1 Y_1 Y_3 Y_4 + \underline{u}_2 (Y_1 Y_3 + Y_3 Y_4 + Y_4 Y_1) + \underline{u}_3 (Y_1 + Y_3 + Y_4) + \underline{u}_4 , \quad (5b)$$

$$\underline{v}_3 K_3 = \underline{u}_1 Y_1 Y_2 Y_4 + \underline{u}_2 (Y_1 Y_2 + Y_2 Y_4 + Y_4 Y_1) + \underline{u}_3 (Y_1 + Y_2 + Y_4) + \underline{u}_4 , \quad (5c)$$

$$\underline{v}_4 K_4 = \underline{u}_1 Y_1 Y_2 Y_3 + \underline{u}_2 (Y_1 Y_2 + Y_2 Y_3 + Y_3 Y_1) + \underline{u}_3 (Y_1 + Y_2 + Y_3) + \underline{u}_4 , \quad (5d)$$

où

$$K_1 = Y_2 Y_3 Y_4 + Y_1 (Y_2 Y_3 + Y_3 Y_4 + Y_4 Y_2) + Y_1^2 (Y_2 + Y_3 + Y_4) + Y_1^3 , \quad (6)$$

et K_2, K_3 et K_4 sont obtenus par permutation circulaire des indices des matrices Y_i.

Dans ce mode de réalisation de l'invention, l'unité de codage 102 transmet ensuite les mots $\underline{v}$ à un entrelaceur 20, qui fournit un « mot entrelacé » $\underline{v}^*$, de longueur 1020, en permutant les symboles du mot

$$\underline{v} = \left(v^0, v^1, \ldots, v^{1019}\right)$$

de la manière suivante :

$$\underline{v}^* = \left(v^0, v^{255}, v^{510}, v^{765}, v^1, v^{256}, v^{511}, v^{766}, \ldots, v^{1019}\right) .$$

Ainsi, une rafale d'erreurs affectant $4b$ symboles de $\underline{v}^*$ en cours de transmission affectera au plus (b+1) symboles dans chacun des mots $\underline{u}_1$, $\underline{u}_2$,

$\underline{u}_3$, et $\underline{u}_4$ (c'est-à-dire (4*b*+4) erreurs en tout), comme on le voit d'après le système d'équations (4), alors qu'en l'absence de l'entrelaceur 20, chacun de ces mots subirait 4*b* erreurs de transmission (c'est-à-dire 16*b* erreurs en tout).

L'entrelaceur 20 transmet ensuite les mots entrelacés $\underline{v}^*$ à un modulateur 103. Ce modulateur 103 associe un symbole de modulation à chaque nombre prédéterminé de symboles binaires (« *bits* »). Puis ces symboles de modulation sont transmis à un enregistreur (ou à un émetteur) 104, qui insère les symboles dans un canal de transmission. Ce canal peut être par exemple un stockage sur un support adapté tel qu'un DVD ou un disque magnétique ou encore une bande magnétique. Il peut correspondre également à une émission filaire ou non-filaire comme c'est le cas d'un lien radio.

Le message transmis, après avoir été affecté par un « bruit de transmission » dont l'effet est de modifier ou d'effacer, aléatoirement, certaines des données transmises, parvient à un lecteur (ou à un récepteur) 105.

Le lecteur (ou récepteur) 105 transmet alors ces symboles élémentaires au démodulateur 106, qui les transforme en symboles de l'alphabet $\mathbf{F}_q$. Dans ce mode de réalisation (où les mots de code $\underline{v}$ sont entrelacés avant transmission), ces symboles reçus sont groupés en « mots reçus entrelacés » $\underline{r}^*$, de longueur 1020, qui sont soumis à un désentrelaceur 30 chargé de transformer chaque mot $\underline{r}^*$ en un « mot reçu » (sous-entendu : désentrelacé) $\underline{r}$, en inversant la permutation opérée par l'entrelaceur 20.

Ce mot $\underline{r}$ est ensuite traité par une unité 107, qui met en œuvre un algorithme de correction d'erreurs destiné à fournir un « mot post-associé »

$$\underline{\hat{u}} = \left[\underline{\hat{u}}_1\, \underline{\hat{u}}_2\, \underline{\hat{u}}_3\, \underline{\hat{u}}_4\right],$$

où les mots $\underline{\hat{u}}_1$, $\underline{\hat{u}}_2$, $\underline{\hat{u}}_3$ et $\underline{\hat{u}}_4$ sont tous de longueur 255, qui est une estimation du mot pré-codé $\underline{u}$.

Selon un mode de réalisation de l'invention, l'unité 107 est adaptée à mettre en œuvre au moins *deux* algorithmes, à savoir :

- un algorithme maximal tel que l'algorithme dit « de Feng-Rao », et
- un algorithme sub-maximal, tel que celui décrit ci-dessous.

Dans ce mode de réalisation, une unité de sélection 40 détermine lequel des deux algorithmes doit être utilisé pour le mot reçu en cours de traitement, en fonction de divers paramètres prédéterminés, qui incluent notamment une évaluation (directe ou indirecte) du bruit du canal.

Si l'unité de sélection 40 détermine que le bruit de transmission courant n'est pas trop élevé, elle commande à l'unité de correction d'erreurs 107 de mettre en œuvre un algorithme sub-maximal (donc moins performant, mais plus économique qu'un algorithme maximal), qui, dans le mode de réalisation considéré ici, opère de la manière suivante.

L'unité de correction d'erreurs 107 calcule d'abord, en partant du mot reçu $\underline{r}$, un « mot post-reçu »

$$\underline{s} = \left[\underline{s}_1\, \underline{s}_2\, \underline{s}_3\, \underline{s}_4\right],$$

où les mots $\underline{s}_1$, $\underline{s}_2$, $\underline{s}_3$ et $\underline{s}_4$ sont tous de longueur 255, que l'on peut interpréter comme étant la version « bruitée » du mot pré-codé $\underline{u}$. Ce mot $\underline{s}$ est donc obtenu (voir le système d'équations (4)) d'après :

$$\begin{aligned}
\underline{s}_1 &= \underline{r}_1 + \underline{r}_2 + \underline{r}_3 + \underline{r}_4, \\
\underline{s}_2 &= \underline{r}_1 Y_1 + \underline{r}_2 Y_2 + \underline{r}_3 Y_3 + \underline{r}_4 Y_4, \\
\underline{s}_3 &= \underline{r}_1 Y_1^2 + \underline{r}_2 Y_2^2 + \underline{r}_3 Y_3^2 + \underline{r}_4 Y_4^2, \\
\underline{s}_4 &= \underline{r}_1 Y_1^3 + \underline{r}_2 Y_2^3 + \underline{r}_3 Y_3^3 + \underline{r}_4 Y_4^3.
\end{aligned} \qquad \text{(7a-d)}$$

Pour obtenir le mot post-associé $\hat{\underline{u}}$, on applique alors indépendamment à chacune de ses quatre composantes un algorithme quelconque apte à corriger les erreurs affectant des mots codés au moyen d'un code de Reed-Solomon. Ainsi, l'on obtient (voir les équations (3a-d)) :

$\hat{\underline{u}}_1$ en corrigeant le mot $\underline{s}_1$ d'après le vecteur de syndromes d'erreurs $H^{(32)} \cdot \underline{s}_1^{\mathrm{T}}$,

$\hat{\underline{u}}_2$ en corrigeant le mot $\underline{s}_2$ d'après le vecteur de syndromes d'erreurs $H^{(28)} \cdot \underline{s}_2^{\mathrm{T}}$,

$\hat{\underline{u}}_3$ en corrigeant le mot $\underline{s}_3$ d'après le vecteur de syndromes d'erreurs $H^{(24)} \cdot \underline{s}_3^{\mathrm{T}}$, et

$\hat{\underline{u}}_4$ en corrigeant le mot $\underline{s}_4$ d'après le vecteur de syndromes d'erreurs $H^{(20)} \cdot \underline{s}_4{}^{\mathrm{T}}$.

Cette quadruple correction d'erreurs est relativement simple et rapide en vertu des qualités des algorithmes connus adaptés aux codes de Reed-Solomon, et ce d'autant plus que l'on corrige des mots de longueur 255 définis sur $\mathbf{F}_{256}$. Comme expliqué ci-dessus, cette plus grande simplicité est la contrepartie d'une réduction du pouvoir de résolution ; plus précisément, compte tenu de la dimension des matrices de parité respectives, on ne pourra corriger ainsi, au mieux, que 16 erreurs dans $\underline{s}_1$, 14 erreurs dans $\underline{s}_2$, 12 erreurs dans $\underline{s}_3$, et 10 erreurs dans $\underline{s}_4$.

Si en revanche le bruit dans le canal est élevé, c'est-à-dire si le taux moyen d'erreurs de transmission dépasse un seuil prédéterminé (l'unité de sélection 40 pourra par exemple déterminer cela en mesurant le nombre d'erreurs corrigées sur un nombre prédéterminé de mots reçus précédents, ou bien en constatant que la tentative de correction, décrite ci-dessus, au moyen de l'algorithme sub-maximal n'a pas abouti), l'unité de sélection 40 commande à l'unité de correction d'erreurs 107 de mettre en œuvre l'algorithme maximal. Plus précisément, l'application de cet algorithme à $\underline{r}$ fournit un mot de code associé à $\underline{r}$, c'est-à-dire une estimation

$$\hat{\underline{v}} = \left[\hat{\underline{v}}_1\, \hat{\underline{v}}_2\, \hat{\underline{v}}_3\, \hat{\underline{v}}_4\right],$$

où les mots $\hat{\underline{v}}_1$, $\hat{\underline{v}}_2$, $\hat{\underline{v}}_3$, et $\hat{\underline{v}}_4$ sont tous de longueur 255, du mot de code $\underline{v}$ transmis. On obtient alors le mot post-associé

$$\hat{\underline{u}} = \left[\hat{\underline{u}}_1\, \hat{\underline{u}}_2\, \hat{\underline{u}}_3\, \hat{\underline{u}}_4\right]$$

d'après les équations :

$$\begin{aligned}
\hat{\underline{u}}_1 &= \hat{\underline{v}}_1 + \hat{\underline{v}}_2 + \hat{\underline{v}}_3 + \hat{\underline{v}}_4, \\
\hat{u}_2 &= \hat{\underline{v}}_1 Y_1 + \hat{\underline{v}}_2 Y_2 + \hat{\underline{v}}_3 Y_3 + \hat{\underline{v}}_4 Y_4, \\
\hat{\underline{u}}_3 &= \hat{\underline{v}}_1 Y^2{}_1 + \hat{\underline{v}}_2 Y^2{}_2 + \hat{\underline{v}}_3 Y^2{}_3 + \hat{\underline{v}}_4 Y^2{}_4, \\
\hat{\underline{u}}_4 &= \hat{\underline{v}}_1 Y^3{}_1 + \hat{\underline{v}}_2 Y^3{}_2 + \hat{\underline{v}}_3 Y^3{}_3 + \hat{\underline{v}}_4 Y^3{}_4.
\end{aligned} \qquad (8a\text{-}d)$$

Dans l'exemple numérique considéré ici, l'algorithme de Feng-Rao peut corriger jusqu'à 40 erreurs dans le mot reçu $\underline{r}$ de longueur 1020. Il fait donc nettement

mieux que l'algorithme sous-maximal, et on fera appel à lui si la qualité de service le requiert, mais en sachant que cet algorithme maximal est complexe, et donc coûteux, ne serait-ce qu'en durée de traitement.

On notera que le taux de codage k/n de ce code de géométrie algébrique est égal à $916/1020$ = 0.898. Un code de Reed-Solomon défini sur $\mathbf{F}_{256}$, de longueur 255 et possédant le même taux de codage aurait une dimension égale à 229, de sorte qu'il faudrait coder les 916 symboles d'information sur quatre mots appartenant à ce code de Reed-Solomon ; la distance minimale de ce code étant égale à 27, on pourra corriger au maximum un nombre d'erreurs égal à 13 dans chacun de ces quatre mots ; on pourra ainsi corriger 52 erreurs en tout, mais seulement dans les cas favorables (0,3 % des cas) où les erreurs sont réparties en nombre égal sur ces quatre mots. Cela est à comparer avec les performances du code selon l'invention qui est capable, comme on l'a dit, de corriger tous les mots contenant au plus 40 erreurs quand on utilise l'algorithme maximal ; quand on utilise l'algorithme sub-maximal, le code selon l'invention est capable d'obtenir correctement $\underline{\hat{u}}_1$ si le mot reçu $\underline{r}$ comporte au plus 16 erreurs, et d'obtenir correctement $\underline{\hat{u}}_2$ si ce mot reçu comporte au plus 14 erreurs, et d'obtenir correctement $\underline{\hat{u}}_3$ si ce mot reçu comporte au plus 12 erreurs, et enfin d'obtenir correctement $\underline{\hat{u}}_4$ si ce mot reçu comporte au plus 10 erreurs. On dit que l'on a affaire ici à un « système de protection inégale contre les erreurs » de transmission (en anglais, « *unequal error protection* » ou UEP).

Une fois la correction terminée, l'unité 107 transmet le mot post-associé $\underline{\hat{u}}$ à une unité de suppression de la redondance 108, qui en extrait k = 916 symboles d'information estimés, en ôtant les symboles de redondance aux positions du mot où l'unité 102 a placé des symboles de redondance au cours du codage. Enfin, ces symboles d'information sont fournis à leur destinataire 109.

On peut considérer que les unités 40, 107 et 108 forment conjointement un « décodeur » 10.

On notera que dans le mode de réalisation décrit ci-dessus, le décodeur 10 fournit une estimation de la totalité des k symboles d'information initialement stockés dans le bloc $\underline{a}$. Mais comme expliqué en introduction, l'invention offre également la possibilité de ne décoder que les symboles d'information contenus dans certaines des (quatre, dans cet exemple) composantes du mot post-associé $\hat{\underline{u}}$: de tels modes de réalisation peuvent être économiquement avantageux pour certaines applications, telles que la transmission d'images codées à la source.

Le schéma synoptique de la **figure 2** représente, de façon très schématique, un appareil d'enregistrement de données d'information 48 incorporant le codeur 102.

Cet appareil 48 comprend un clavier 911, un écran 909, une source d'informations externe 100, un modulateur 103 et un enregistreur de données modulées 104, conjointement reliés à des ports d'entrée/sortie 903 d'un dispositif de codage 102 qui est réalisé ici sous la forme d'une unité logique.

Le dispositif de codage 102 comporte, reliés entre eux par un bus d'adresses et de données 902 :

- une unité centrale de traitement 900,
- une mémoire vive RAM 904,
- une mémoire morte 905, et
- lesdits ports d'entrée/sortie 903.

Chacun des éléments illustrés en figure 2 est bien connu de l'homme du métier des micro-ordinateurs et des systèmes de transmission et, plus généralement, des systèmes de traitement de l'information. Ces éléments connus ne sont donc pas décrits ici. On observe, cependant, que :

- la source d'informations 100 pourrait être, par exemple, un périphérique d'interface, un capteur, un démodulateur, une mémoire externe ou un autre système de traitement de l'information (non représenté), et pourrait par exemple fournir des séquences de signaux représentatifs de parole, de messages de service ou de données multimédia notamment de type IP ou ATM, sous forme de séquences de données binaires, et

- l'enregistreur 104 est adapté à enregistrer des données modulées sur un support tel qu'un disque magnétique.

La mémoire vive 904 conserve des données, des variables et des résultats intermédiaires de traitement, dans des registres de mémoire portant, dans la description, les mêmes noms que les données dont ils conservent les valeurs. On observera, au passage, que le mot « registre » désigne, à travers la présente description, aussi bien une zone mémoire de faible capacité (quelques données binaires) qu'une zone mémoire de grande capacité (permettant de stocker un programme entier) au sein d'une mémoire vive ou d'une mémoire morte.

La mémoire vive 904 comporte notamment les registres suivants :

- un registre « *symboles_information* » dans lequel sont conservés les symboles d'information appartenant à $\mathbf{F}_q$,

- un registre « *mots_précodés* », dans lequel sont conservés les mots $\underline{u}$, et

- un registre « *mots_code* », dans lequel sont conservés les mots de code $\underline{v}$ avant qu'ils ne soient soumis au modulateur 103.

La mémoire morte 905 est adaptée à conserver, dans des registres qui, par commodité, possèdent les mêmes noms que les données qu'ils conservent :

- le programme de fonctionnement de l'unité centrale de traitement 900, dans un registre « programme »,

- la longueur des mots de code enregistrés, dans un registre « *longueur_mots* »,

- le cardinal du corps de Galois $\mathbf{F}_q$ servant d'alphabet pour le code utilisé, dans un registre « q »,

- le nombre de symboles d'information servant à construire un mot de code, dans un registre « k », et

- la matrice de parité du code, dans un registre « H ».

Le schéma synoptique de la **figure 3** représente, de façon très schématique, un appareil de reproduction de données d'information 70 incorporant le décodeur 10.

Cet appareil 70 comprend un clavier 711, un écran 709, un destinataire d'informations externe 109, un lecteur de données modulées 105 et un démodulateur 106, conjointement reliés à des ports d'entrée/sortie 703 du décodeur 10 qui est réalisé ici sous la forme d'une unité logique.

Le décodeur 10 comporte, reliés entre eux par un bus d'adresses et de données 702 :

- une unité centrale de traitement 700,
- une mémoire vive (RAM) 704,
- une mémoire morte (ROM) 705, et
- lesdits ports d'entrée/sortie 703.

Chacun des éléments illustrés en figure 3 est bien connu de l'homme du métier des micro-ordinateurs et des systèmes de transmission et, plus généralement, des systèmes de traitement de l'information. Ces éléments connus ne sont donc pas décrits ici. On observe, cependant, que :

- le destinataire d'informations 109 pourrait être, par exemple, un périphérique d'interface, un afficheur, un modulateur, une mémoire externe ou un autre système de traitement de l'information (non représenté), et pourrait être adapté à recevoir des séquences de signaux représentatifs de parole, de messages de service ou de données multimédia notamment de type IP ou ATM, sous forme de séquences de données binaires, et
- le lecteur 105 est adapté à lire des données modulées enregistrées sur un support tel qu'un disque magnétique.

La mémoire vive 704 conserve des données, des variables et des résultats intermédiaires de traitement, dans des registres de mémoire portant, dans la description, les mêmes noms que les données dont ils conservent les valeurs. La mémoire vive 704 comporte notamment les registres suivants :

- un registre « *mots_reçus* », dans lesquels sont conservés les mots reçus $\underline{r}$,
- un registre « *mots_associés* », dans lequel sont conservés, le cas échéant, les mots $\underline{\hat{v}}$ résultant de la correction de $\underline{r}$ par l'algorithme maximal,
- un registre « *mots_postreçus* », dans lequel sont conservés, le cas échéant, les mots $\underline{s}$ obtenus à partir de $\underline{r}$ au moyen des équations (7a-d),

- un registre « *mots_postassociés* », dans lequel sont conservés les mots $\hat{\underline{u}}$ résultant de la mise en œuvre soit de l'algorithme maximal, soit des algorithmes sub-maximaux, et

- un registre « *symboles_information* », dans lequel sont conservés les symboles résultant de la suppression de la redondance.

La mémoire morte 705 est adaptée à conserver, dans des registres qui, par commodité, possèdent les mêmes noms que les données qu'ils conservent :

- le programme de fonctionnement de l'unité centrale de traitement 700, dans un registre « programme »,

- la longueur des blocs de données transmises, dans un registre « *longueur_blocs* »,

- le cardinal du corps de Galois $\mathbf{F}_q$ servant d'alphabet pour le code utilisé, dans un registre « q »,

- le nombre de symboles d'information servant à construire un mot de code, dans un registre « k », et

- la matrice de parité du code, dans un registre « H ».

On notera que, dans certaines applications, il sera commode d'utiliser le même dispositif informatique (fonctionnant en mode multi-tâches) pour l'échange, c'est-à-dire à la fois l'émission et la réception, de signaux selon l'invention ; dans ce cas, les unités 10 et 102 seront physiquement identiques.

On a décrit ci-dessus à titre d'exemple une application de l'invention au stockage de masse des données, mais il est clair que les procédés selon l'invention peuvent tout aussi bien être mis en œuvre au sein d'un réseau de télécommunications, auquel cas l'unité 105 par exemple pourrait être un récepteur adapté à mettre en œuvre un protocole de transmission de données par paquets sur un canal hertzien.

REVENDICATIONS

1. Procédé de codage de symboles d'information selon un code défini sur un corps de Galois $\mathbf{F}_q$, où q est un entier supérieur à 2 et égal à une puissance d'un nombre premier, et de longueur $n = p(q-1)$, où p un entier supérieur à 1, caractérisé en ce qu'il comprend les étapes suivantes :

a) on choisit un p-uple d'entiers $(t_1,\ldots,t_p)$ tels que

$q-1 > t_1 > t_2 > \ldots > t_p > 0$,

et un p-uple de matrices carrées diagonales $(Y_1,\ldots,Y_p)$ de dimension $(q-1)$ sur $\mathbf{F}_q$ telles que, pour tout i $(1 \leq i \leq q-1)$, les p éléments en position (i,i) de ces matrices $Y_1,\ldots,Y_p$ sont différents deux à deux,

b) on place lesdits symboles d'information successivement dans p mots $\underline{a}_l$ de longueur $(q-1-t_l)$ (où $l = 1,\ldots,p$),

c) on forme des mots $\underline{u}_l$ (où $l = 1,\ldots,p$) de longueur $(q-1)$, qui constituent les composantes du « mot pré-codé » $\underline{u} = [\underline{u}_1\ \underline{u}_2\ \ldots\ \underline{u}_p]$, en complétant le mot $\underline{a}_l$ correspondant au moyen de symboles de redondance de manière à ce que $\underline{u}_l$ soit orthogonal à la matrice $H^{(t_l)}$, où les matrices $H^{(t)}$ sont définies par $H^{(t)}_{ij} = \gamma^{i(j-1)}$ $(1 \leq i \leq t,\ 1 \leq j \leq q-1)$, où γ est un symbole choisi parmi les éléments primitifs de $\mathbf{F}_q$, et

d) on forme un mot de code

$\underline{v} = [\underline{v}_1\ \underline{v}_2\ \ldots\ \underline{v}_p]$,

où chaque mot $\underline{v}_l$ $(l = 1,\ldots,p)$ est de longueur $(q-1)$, en résolvant le système d'équations

$$\begin{cases} \underline{v}_1 + \underline{v}_2 + \ldots + \underline{v}_p = \underline{u}_1 , \\ \underline{v}_1 Y_1 + \underline{v}_2 Y_2 + \ldots + \underline{v}_p Y_p = \underline{u}_2 , \\ \underline{v}_1 Y_1^2 + \underline{v}_2 Y_2^2 + \ldots + \underline{v}_p Y_p^2 = \underline{u}_3 , \\ \qquad\qquad \ldots \\ \underline{v}_1 Y_1^{p-1} + \underline{v}_2 Y_2^{p-1} + \ldots + \underline{v}_p Y_p^{p-1} = \underline{u}_p . \end{cases}$$

2. Procédé de codage selon la revendication 1, caractérisé en ce que l'on considère une équation algébrique en X et Y telle que, pour toute valeur γ^{i-1} (i = 1,...,q−1) prise par X, ladite équation algébrique possède p solutions distinctes notées $y_l(\gamma^{i-1})$ (où l = 1,...,p), et en ce que l'élément diagonal en position (i,i) de chacune desdites matrices Y_l est pris égal à $y_l(\gamma^{i-1})$.

3. Procédé de codage selon la revendication 1 ou la revendication 2, caractérisé en ce que chaque mot $\underline{a}_l$ (où l = 1,...,p) représente une approximation de résolution respective d'une image codée à la source.

4. Procédé de décodage de données reçues résultant de la transmission de symboles codés selon la revendication 1, caractérisé en ce qu'il comprend les étapes suivantes :

e) on calcule, à partir du mot reçu

$$\underline{r} = [\underline{r}_1\ \underline{r}_2\ \cdots\ \underline{r}_p]\ ,$$

où chaque mot $\underline{r}_l$ (l = 1,...,p) est de longueur (q−1), au moins une des composantes $\underline{s}_l$ (où l = 1,...,p) de longueur (q−1), du « mot post-reçu » $\underline{s} = [\underline{s}_1\ \underline{s}_2\ \cdots\ \underline{s}_p]$, d'après :

$$\begin{cases} \underline{s}_1 = \underline{r}_1 + \underline{r}_2 + \cdots + \underline{r}_p\ , \\ \underline{s}_2 = \underline{r}_1 Y_1 + \underline{r}_2 Y_2 + \cdots + \underline{r}_p Y_p\ , \\ \underline{s}_3 = \underline{r}_1 Y_1^2 + \underline{r}_2 Y_2^2 + \cdots + \underline{r}_p Y_p^2\ , \\ \qquad\qquad \cdots \\ \underline{s}_p = \underline{r}_1 Y_1^{p-1} + \underline{r}_2 Y_2^{p-1} + \cdots + \underline{r}_p Y_p^{p-1}\ , \end{cases}$$

et

f) on calcule au moins une des composantes $\hat{\underline{u}}_l$ (où l = 1,...,p), de longueur (q−1), du « mot post-associé » $\hat{\underline{u}} = [\hat{\underline{u}}_1 \hat{\underline{u}}_2 \ldots \hat{\underline{u}}_p]$, en corrigeant le mot $\underline{s}_l$ de même l d'après le vecteur de syndromes d'erreurs $H^{(t_l)} \cdot \underline{s}_l{}^{\mathrm{T}}$.

5. Procédé de décodage de données reçues résultant de la transmission de symboles codés selon la revendication 2, caractérisé en ce qu'il comprend les étapes suivantes :

e') on applique à chaque mot reçu $\underline{r}$ un algorithme de correction d'erreurs maximal, de manière à obtenir une estimation

$\underline{\hat{v}} = [\underline{\hat{v}}_1\ \underline{\hat{v}}_2\ \cdots\ \underline{\hat{v}}_p]$,

où chaque mot $\underline{\hat{v}}_l$ (l = 1,...,p) est de longueur (q−1), du mot transmis $\underline{v}$ correspondant, et

f') on calcule au moins une des composantes $\underline{\hat{u}}_l$ (où l = 1,...,p), de longueur (q−1), du « mot post-associé » $\underline{\hat{u}} = [\underline{\hat{u}}_1 \underline{\hat{u}}_2 ... \underline{\hat{u}}_p]$, d'après :

$$\begin{cases} \underline{\hat{u}}_1 = \underline{\hat{v}}_1 + \underline{\hat{v}}_2 + \ldots + \underline{\hat{v}}_p , \\ \underline{\hat{u}}_2 = \underline{\hat{v}}_1 Y_1 + \underline{\hat{v}}_2 Y_2 + \ldots + \underline{\hat{v}}_p Y_p , \\ \underline{\hat{u}}_3 = \underline{\hat{v}}_1 Y_1^2 + \underline{\hat{v}}_2 Y_2^2 + \ldots + \underline{\hat{v}}_p Y_p^2 , \\ \qquad\qquad \ldots \\ \underline{\hat{u}}_p = \underline{\hat{v}}_1 Y_1^{p-1} + \underline{\hat{v}}_2 Y_2^{p-1} + \ldots + \underline{\hat{v}}_p Y_p^{p-1} . \end{cases}$$

6. Procédé de décodage de données reçues résultant de la transmission de symboles codés selon la revendication 2, caractérisé en ce qu'il comprend une étape préliminaire consistant à choisir, pour le mot reçu courant, entre les étapes du procédé selon la revendication 4, et les étapes du procédé selon la revendication 5, en fonction de critères prédéterminés.

7. Procédé de décodage de données reçues résultant de la transmission de symboles codés selon la revendication 2, caractérisé en ce que, pour tout mot reçu, on met d'abord en œuvre un algorithme de correction d'erreurs selon la revendication 4, et en ce que, au cas où cet algorithme n'aboutit pas, on déclare qu'une erreur non corrigible a été détectée.

8. Procédé de décodage de données reçues résultant de la transmission de symboles codés selon la revendication 2, caractérisé en ce que, pour tout mot reçu, on met d'abord en œuvre un algorithme de correction d'erreurs selon la revendication 4, et en ce que, au cas où cet algorithme n'aboutit pas, on met ensuite en œuvre un algorithme de correction d'erreurs selon la revendication 5.

9. Procédé de décodage selon l'une quelconque des revendications 4 à 8, caractérisé en ce qu'il comprend en outre l'étape consistant à obtenir des symboles d'information estimés en ôtant d'au moins une composante $\underline{\hat{u}}_l$ (l = 1,...,p) les symboles situés aux positions identiques aux positions de la composante $\underline{u}_l$ de même l du mot pré-codé $\underline{u}$ correspondant, dans lesquelles

des symboles de redondance ont été placés à l'étape c) du procédé selon la revendication 1.

10. Procédé de communication de symboles d'information comprenant les étapes suivantes :

1) on code lesdits symboles d'information conformément à un procédé de codage selon la revendication 1, de façon à former des mots de code $\underline{v} = \left(v^0, v^1, \ldots, v^{n-1}\right)$,

2) on permute les symboles de chaque mot de code $\underline{v}$ de façon à former un mot à transmettre

$$\underline{v}^* = \left(v^0, v^{q-1}, v^{2(q-1)}, \ldots, v^{(p-1)(q-1)}, v^1, v^q, v^{2q-1}, \ldots, v^{(p-1)(q-1)+1}, \ldots, v^{n-1}\right),$$

3) on transmet ledit mot $\underline{v}^*$,

4) on reçoit un mot entrelacé

$$\underline{r}^* = \left(r^0, r^{q-1}, r^{2(q-1)}, \ldots, r^{(p-1)(q-1)}, r^1, r^q, v^{2q-1}, \ldots, r^{(p-1)(q-1)+1}, \ldots, r^{n-1}\right),$$

correspondant au mot $\underline{v}^*$,

5) on permute les symboles du mot entrelacé $\underline{r}^*$ de façon à former un mot reçu $\underline{r} = \left(r^0, r^1, \ldots, r^{n-1}\right)$, et

6) on décode le mot reçu $\underline{r}$ conformément à un procédé de décodage selon la revendication 4 ou la revendication 5.

11. Dispositif de codage (102) de symboles d'information selon un code défini sur un corps de Galois $\mathbf{F}_q$, où q est un entier supérieur à 2 et égal à une puissance d'un nombre premier, et de longueur $n = p(q-1)$, où p un entier supérieur à 1, caractérisé en ce que, un p-uple d'entiers $(t_1,\ldots,t_p)$ tels que

$q-1 > t_1 > t_2 > \ldots > t_p > 0$,

et un p-uple de matrices carrées diagonales $(Y_1,\ldots,Y_p)$ de dimension $(q-1)$ sur $\mathbf{F}_q$ telles que, pour tout i ($1 \leq i \leq q-1$), les p éléments en position (i,i) de ces matrices $Y_1,\ldots,Y_p$ sont différents deux à deux, ayant été choisis, il est apte :

- à placer lesdits symboles d'information successivement dans p mots $\underline{a}_l$ de longueur $(q-1-t_l)$ (où $l = 1,\ldots,p$),

- à former des mots $\underline{u}_l$ (où $l = 1,\ldots,p$) de longueur $(q-1)$, qui constituent les composantes du « mot pré-codé » $\underline{u} = [\underline{u}_1\ \underline{u}_2\ \ldots\ \underline{u}_p]$, en complétant le mot $\underline{a}_l$ correspondant au moyen de symboles de redondance de manière à ce que $\underline{u}_l$ soit orthogonal à la matrice $H^{(t_l)}$, où les matrices $H^{(t)}$ sont définies par $H^{(t)}_{ij} = \gamma^{i(j-1)}$ $(1 \leq i \leq t,\ 1 \leq j \leq q-1)$, où γ est un symbole choisi parmi les éléments primitifs de $\mathbf{F}_q$, et

- à former un mot de code

$$\underline{v} = [\underline{v}_1\ \underline{v}_2\ \cdots\ \underline{v}_p]\ ,$$

où chaque mot $\underline{v}_l$ $(l = 1,\ldots,p)$ est de longueur $(q-1)$, en résolvant le système d'équations

$$\begin{cases} \underline{v}_1 + \underline{v}_2 + \ldots + \underline{v}_p = \underline{u}_1\ , \\ \underline{v}_1 Y_1 + \underline{v}_2 Y_2 + \ldots + \underline{v}_p Y_p = \underline{u}_2\ , \\ \underline{v}_1 Y_1^2 + \underline{v}_2 Y_2^2 + \ldots + \underline{v}_p Y_p^2 = \underline{u}_3\ , \\ \qquad\qquad \ldots \\ \underline{v}_1 Y_1^{p-1} + \underline{v}_2 Y_2^{p-1} + \ldots + \underline{v}_p Y_p^{p-1} = \underline{u}_p\ . \end{cases}$$

12. Dispositif de codage selon la revendication 11, caractérisé en ce qu'il est en outre apte à assigner la valeur y_l (γ^{i-1}) à l'élément diagonal en position (i,i) de chacune desdites matrices Y_l, où, pour une équation algébrique en X et Y prédéterminée, ladite équation algébrique possède p solutions distinctes notées $y_l(\gamma^{i-1})$ (où $l = 1,\ldots,p$) pour toute valeur γ^{i-1} $(i = 1,\ldots,q-1)$ prise par X.

13. Dispositif de décodage (10) de mots reçus $\underline{r}$ résultant de la transmission de mots $\underline{v}$ codés selon la revendication 1, caractérisé en ce qu'il comprend :

- une unité de correction d'erreurs (107) apte à appliquer à chaque mot reçu $\underline{r}$ un algorithme de correction d'erreurs, de manière à fournir au moins une composante $\hat{\underline{u}}_l$ (où $l = 1,\ldots,p$) d'un « mot post-associé » $\hat{\underline{u}}$, et

- une unité de suppression de la redondance (108) apte à ôter de ladite composante $\hat{\underline{u}}_l$ les symboles situés aux positions identiques aux positions de la

composante $\underline{u}_l$ de même l du mot pré-codé $\underline{u}$ correspondant, dans lesquelles des symboles de redondance ont été placés lors du codage.

14. Dispositif de décodage de mots reçus $\underline{r}$ résultant de la transmission de mots $\underline{v}$ codés selon la revendication 2, caractérisé en ce qu'il comprend :

- une unité de sélection (40) capable de déterminer, en fonction de critères prédéterminés, si l'on doit appliquer au mot reçu $\underline{r}$ courant les étapes du procédé selon la revendication 4, et/ou les étapes du procédé selon la revendication 5,

- une unité de correction d'erreurs (107) apte à appliquer à chaque mot reçu $\underline{r}$ un algorithme de correction d'erreurs, de manière à fournir au moins une composante $\hat{\underline{u}}_l$ (où $l = 1,\ldots,p$) d'un « mot post-associé » $\hat{\underline{u}}$, et

- une unité de suppression de la redondance (108) apte à ôter de ladite composante $\hat{\underline{u}}_l$ les symboles situés aux positions identiques aux positions de la composante $\underline{u}_l$ de même l du mot pré-codé $\underline{u}$ correspondant dans lesquelles des symboles de redondance ont été placés lors du codage.

15. Appareil (48) de transmission de données d'information, caractérisé en ce qu'il comprend un dispositif de codage selon la revendication 11 ou la revendication 12, ainsi qu'un modulateur (103) pour moduler les données résultant du codage desdites données d'information.

16. Appareil (70) de réception de données, caractérisé en ce qu'il comprend un démodulateur (106) pour démoduler les données reçues, ainsi qu'un dispositif de décodage selon la revendication 13 ou la revendication 14.

17. Appareil de transmission (48) de données d'information, caractérisé en ce qu'il comprend un dispositif de codage selon la revendication 11 ou la revendication 12, un entrelaceur (20) apte à permuter les symboles de chaque mot de code $\underline{v} = \left(v^0, v^1, \ldots, v^{n-1}\right)$ de façon à former un mot à transmettre

$$\underline{v}^* = \left(v^0, v^{q-1}, v^{2(q-1)}, \ldots, v^{(p-1)(q-1)}, v^1, v^q, v^{2q-1}, \ldots, v^{(p-1)(q-1)+1}, \ldots, v^{n-1}\right),$$

et un modulateur (103) pour moduler les symboles dudit mot à transmettre $\underline{v}^*$.

18. Appareil (70) de réception de données, caractérisé en ce qu'il comprend un démodulateur (106) pour démoduler les données reçues de façon à former des mots reçus entrelacés

$$\underline{r}^* = \left(r^0, r^{q-1}, r^{2(q-1)}, \ldots, r^{(p-1)(q-1)}, r^1, r^q, v^{2q-1}, \ldots, r^{(p-1)(q-1)+1}, \ldots, r^{n-1}\right),$$

où q est un entier supérieur à 2 et égal à une puissance d'un nombre premier, p un entier supérieur à 1, et $n = p(q-1)$, un désentrelaceur (30) pour permuter les symboles de chaque mot reçu entrelacé $\underline{r}^*$ de façon à former un mot reçu $\underline{r} = \left(r^0, r^1, \ldots, r^{n-1}\right)$, et un dispositif de décodage selon la revendication 13 ou la revendication 14.

19. Moyen de stockage de données inamovible, caractérisé en ce qu'il comporte des instructions de code de programme informatique pour l'exécution des étapes d'un procédé de codage selon l'une quelconque des revendications 1 à 3, et/ou d'un procédé de décodage selon l'une quelconque des revendications 4 à 9, et/ou d'un procédé de communication selon la revendication 10.

20. Moyen de stockage de données partiellement ou totalement amovible, caractérisé en ce qu'il comporte des instructions de code de programme informatique pour l'exécution des étapes d'un procédé de codage selon l'une quelconque des revendications 1 à 3, et/ou d'un procédé de décodage selon l'une quelconque des revendications 4 à 9, et/ou d'un procédé de communication selon la revendication 10.

21. Programme d'ordinateur, caractérisé en ce qu'il contient des instructions telles que, lorsque ledit programme commande un dispositif de traitement de données programmable, lesdites instructions font que ledit dispositif de traitement de données met en œuvre un procédé de codage selon l'une quelconque des revendications 1 à 3, et/ou d'un procédé de décodage selon l'une quelconque des revendications 4 à 9, et/ou d'un procédé de communication selon la revendication 10.

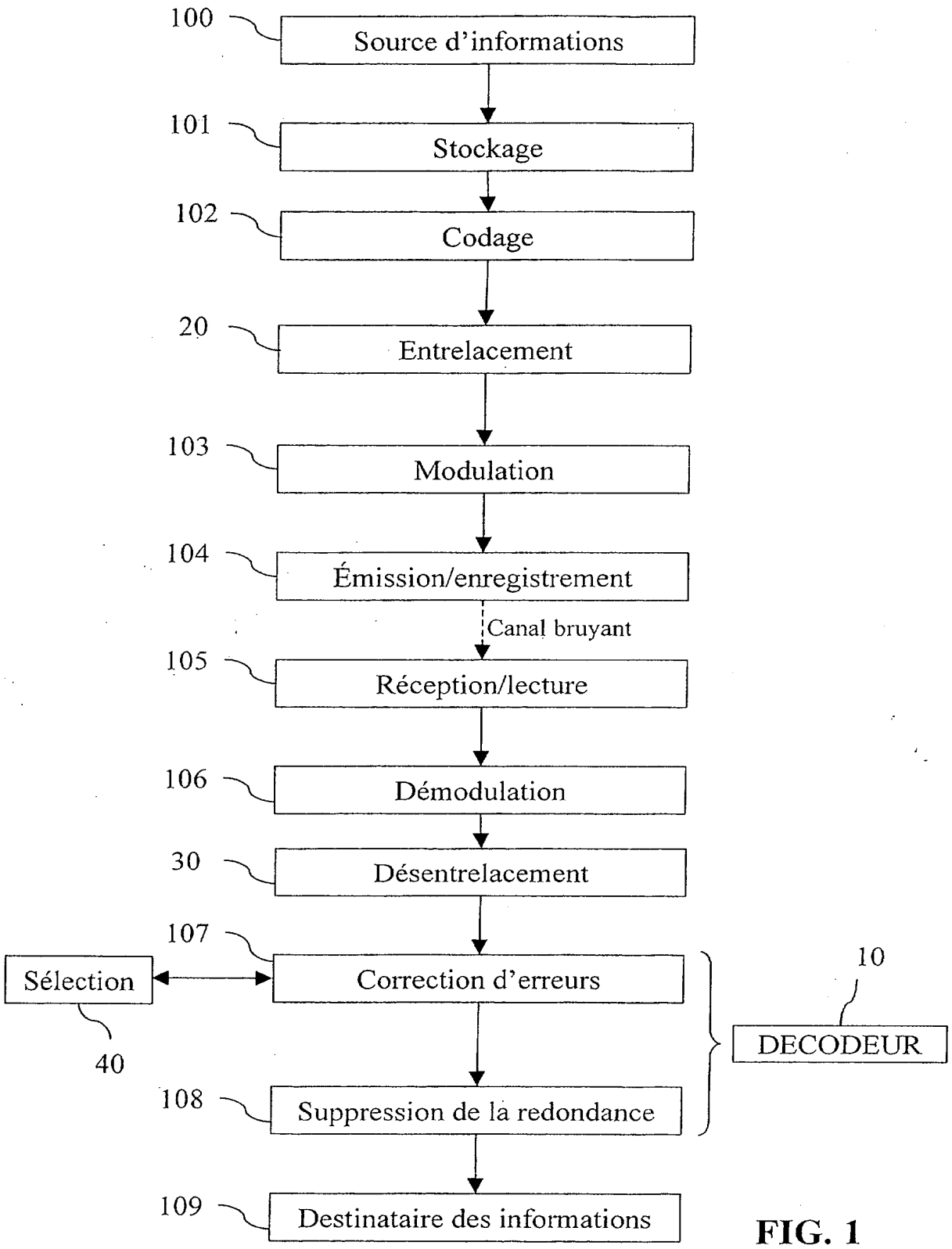

100
Source d'informations
101
Stockage
102
Codage
20
Entrelacement
103
Modulation
104
Émission/enregistrement
Canal bruyant
105
Réception/lecture
106
Démodulation
30
Désentrelacement
107
Sélection
Correction d'erreurs
40
10
DECODEUR
108
Suppression de la redondance
109
Destinataire des informations

FIG. 1

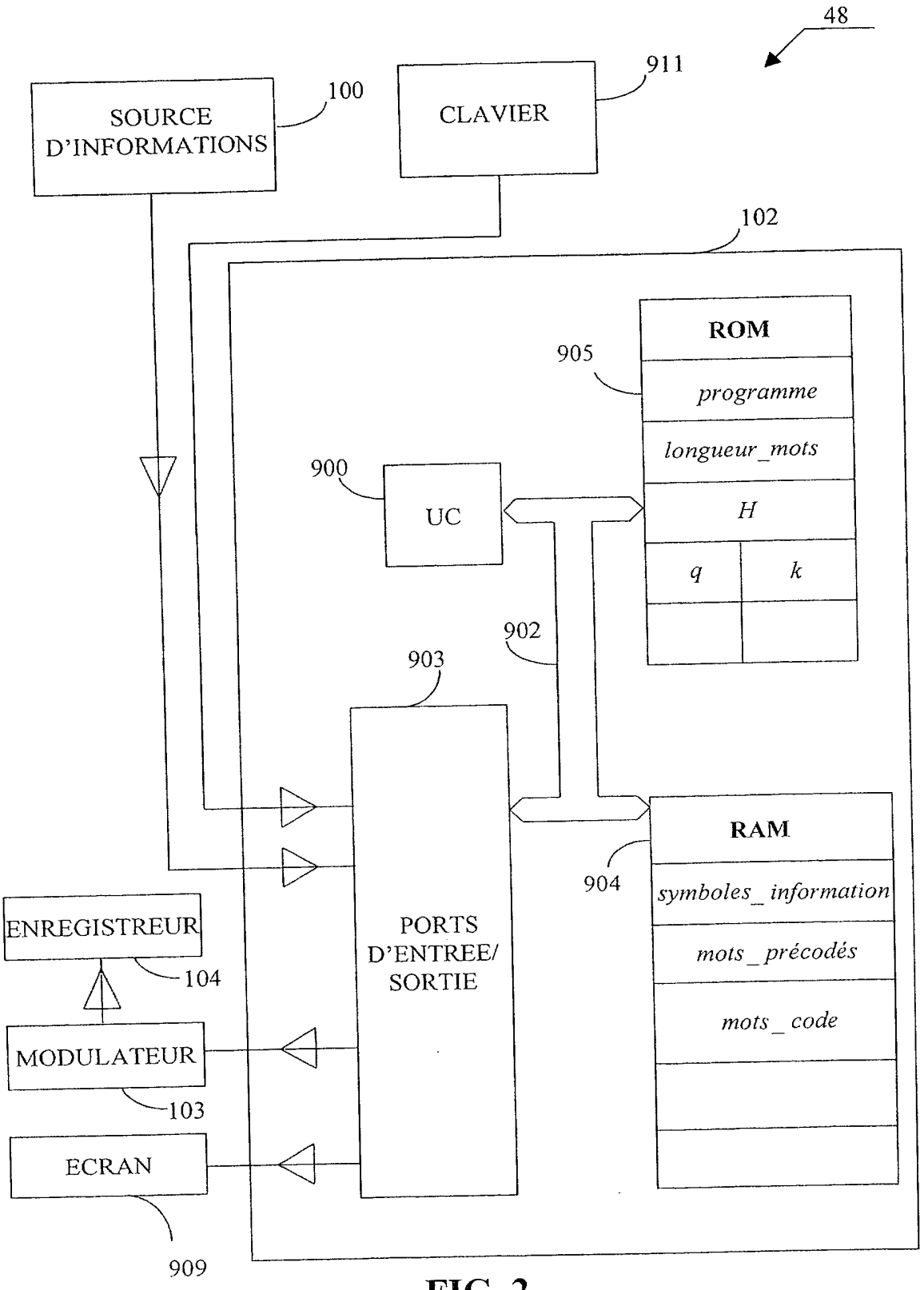

48
SOURCE D'INFORMATIONS
100
CLAVIER
911
102
ROM
905
programme
longueur_mots
H
q
k
900
UC
902
903
RAM
904
symboles_information
mots_précodés
mots_code
PORTS D'ENTREE/ SORTIE
ENREGISTREUR
104
MODULATEUR
103
ECRAN
909

FIG. 2

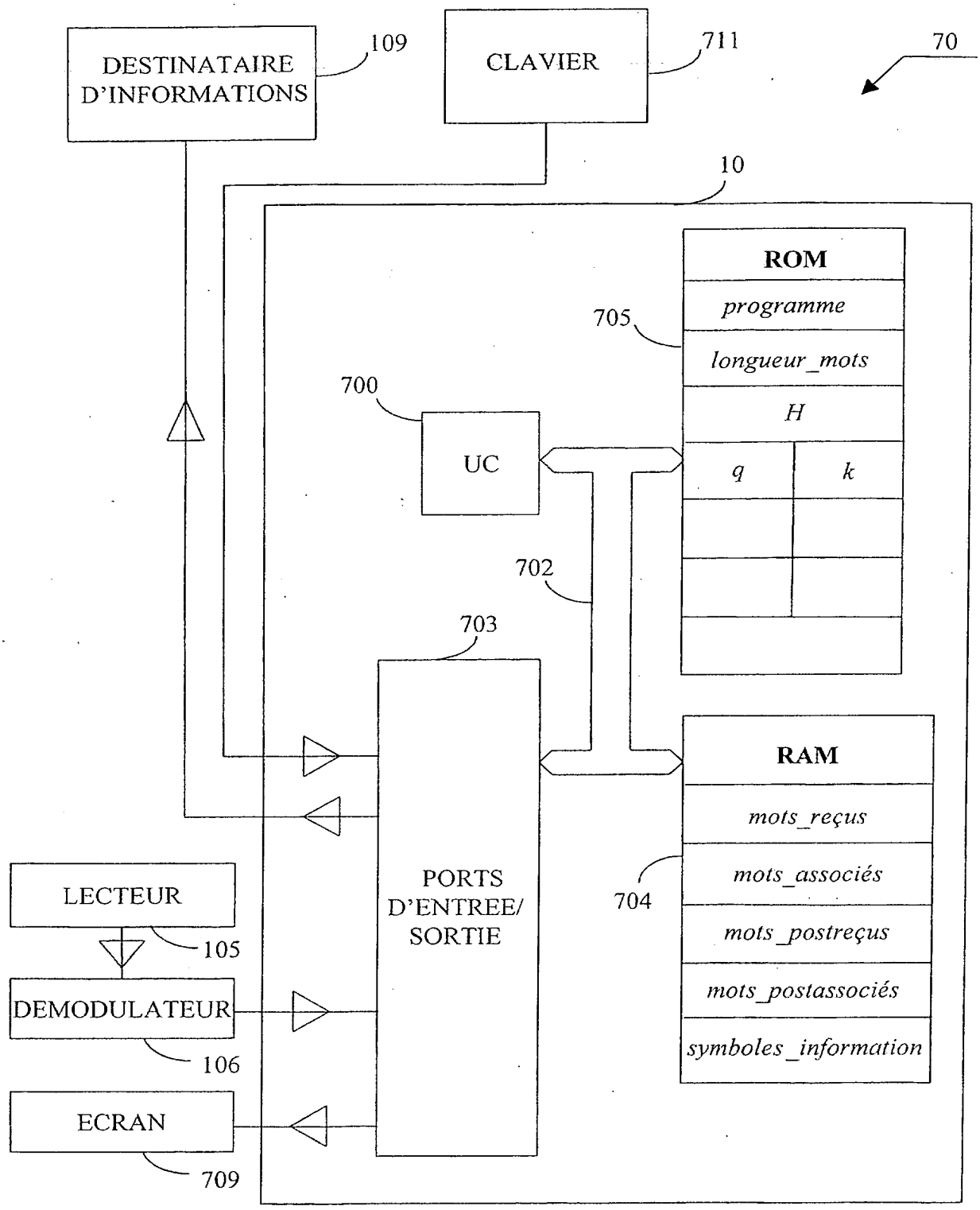

DESTINATAIRE D'INFORMATIONS
109
CLAVIER
711
70
10
ROM
programme
705
longueur_mots
H
700
UC
q
k
702
703
RAM
mots_reçus
mots_associés
704
mots_postreçus
mots_postassociés
symboles_information
PORTS D'ENTREE/ SORTIE
LECTEUR
105
DEMODULATEUR
106
ECRAN
709

FIG. 3

reçue le 03/06/03

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*03

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

INV

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 270601

Vos références pour ce dossier *(facultatif)*	BIF023276/DM/LJH
N° D'ENREGISTREMENT NATIONAL	0304766

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Codage d'informations par code de géométrie algébrique offrant deux options de décodage.

LE(S) DEMANDEUR(S) :

CANON KABUSHIKI KAISHA

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1 Nom		PIRET
Prénoms		Philippe
Adresse	Rue	4, Boulevard des Métairies,
	Code postal et ville	35510 CESSON-SEVIGNE, France
Société d'appartenance *(facultatif)*		
2 Nom		LEHOBEY
Prénoms		Frédéric
Adresse	Rue	185, rue de Fougères,
	Code postal et ville	35700 RENNES, France
Société d'appartenance *(facultatif)*		
3 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

Le 16 avril 2003
Bruno QUANTIN N° 92.1206
SANTARELLI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.